REMARKS / ARGUMENTS

Status of Claims

Claims 1-11, 21-31, and 41-51 are pending in the application. Claims 1-11, 21-31, and 41-51 stand rejected. Applicant has amended Claims 1, 21 and 41 leaving Claims 1-11, 21-31, and 41-51 for consideration upon entry of the present Amendment.

Applicant respectfully submits that the rejection under 35 U.S.C. §103 (a) has been traversed, that no new matter has been entered, and that the application is in condition for allowance.

First Rejection Under 35 U.S.C. §103(a)

Claims 1-5, 7-9, 21-25, 27-29, 41-45 and 47-49 were rejected under 35 U.S.C. 103(a) as being unpatentable over Scott Oaks (hereinafter referred as Scott) (Java Security May 2001 XP002321663) in view of Lee, et al. (hereinafter referred to as Lee) U.S. Pub No. 2002/0147763 A1. Applicants respectfully traverse this rejection.

"A patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007). To find obviousness, the Examiner must "identify a reason that would have prompted a person of ordinary skill in the art in the relevant field to combine the elements in the way the claimed new invention does." *Id.*

Claim 1 as amended, recites "A method for running a tamper-resistant application in a trusted environment, comprising: defining a trusted virtual machine environment that contains a trusted dictionary for protecting data, wherein the trusted dictionary having an associated secure count, comprises a subclass of a standard base class dictionary using any class that allows a storing and a retrieving of data values, wherein the trusted dictionary contains keywords and values encrypted with a secret including a key, and wherein the trusted dictionary includes a list of public keys, wherein each time the secure count is

incremented during operation of the application, the trusted dictionary is placed into an irreversible state, such that the trusted dictionary cannot be placed into a pervious state by replacing a file associated with the trusted dictionary with an older version of the file; verifying the integrity of the application; wherein, if the application is tampered with, the trusted virtual machine environment prevents the application from accessing the secret in the trusted dictionary, and further prevents changing of the trusted dictionary to the previous state, thus disabling the normal operation of the application." (Emphasis Added)

It is respectfully submitted that Scott in view of Lee does not teach, suggest or otherwise disclose a trusted dictionary "having an associated secure count…wherein each time the secure count is incremented during operation of the application, the trusted dictionary is placed into an irreversible state, such that the trusted dictionary cannot be placed into a pervious state by replacing a file associated with the trusted dictionary with an older version of the file…and further prevents changing of the trusted dictionary to the previous state".

Instead, Applicants continue to respectfully point out that the passages cited by the Examiner describe signed classes. Scott indicates that one of the primary applications of digital signatures in Java is to create and verify signed classes. More specifically, a policy file can insist that classes coming from a particular site be signed by a particular entity before the access controller will grant that particular set of permissions. Scott states that the security manager can cooperate with the class loader in order to determine whether or not a particular class is signed. The security manager is then free to grant permissions to that class based upon its own internal policy. The digital signatures are created and verified by using a jarsigner utility to create the signed class. A class loader knows how to understand the digital signature associated with the class. A security manager or access controller then grants the desired permissions based upon the digital signature.

In addition, Lee teaches a Smart Generator that allows the designer/developer/user to model the EJB components in a natural way without being concerned with implementation-specific details. The developer models the business objects using a UML

drawing tool and the Smart Generator creates a set of classes that implements these objects with reference to the Enterprise JavaBeans specification. That is, the Smart Generator automatically creates access methods and handling containment of references from the UML diagram. While Lee does disclose a Template Dictionary, Lee does not disclose a Trusted Dictionary "having an associated secure count…wherein each time the secure count is incremented during operation of the application, the trusted dictionary is placed into an irreversible state, such that the trusted dictionary cannot be placed into a pervious state by replacing a file associated with the trusted dictionary with an older version of the file…and further prevents changing of the trusted dictionary to the previous state", as in Applicants' claimed invention.

In view of the foregoing considerations, it is submitted that Claims 1, 21, and 41 is patentable over Scott in view of Lee. It is further submitted that Claims 1, 21, and 41 are allowable over the prior art of record. Dependent claims inherit all limitations of the corresponding base claim and any intervening claims. Thus, since Claims 2-11 depend from claim 1, it is submitted that, as a matter of law, Claims 2-11 are allowable because claims 2-11 depend from an allowable base claim. Similarly, since Claims 22-31 depend from Claim 21, it is submitted that, as a matter of law, Claims 22-31 are allowable because Claims 22-31 depend from an allowable base claim. Moreover, since Claims 42-51 depend from Claim 41, it is submitted that, as a matter of law, Claims 42-51 are allowable because Claims 42-51 depend from an allowable base claim.

Second Rejection Under 35 U.S.C. §103(a)

Claims 6, 26, 46 were rejected under 35 U.S.C. 103(a) as being unpatentable over Scott Oaks (hereinafter referred as Scott) (Java Security May 2001 XP002321663) in view of Lee, et al. (hereinafter referred to as Lee) U.S. Pub No. 2002/0147763 A1 and further in view of Levy, et al (hereinafter referred as Levy) US Patent No. 6,092,147. Applicants respectfully traverse this rejection. Claim 6 depends from independent claim 1, whereas Claim 26 depends from independent Claim 21 and Claim 46 depends from independent Claim 41. As indicated above, Claims 1, 21 and 41

have been amended to recite, inter alia, a Trusted Dictionary "having an associated secure count…wherein each time the secure count is incremented during operation of the application, the trusted dictionary is placed into an irreversible state, such that the trusted dictionary cannot be placed into a pervious state by replacing a file associated with the trusted dictionary with an older version of the file…and further prevents changing of the trusted dictionary to the previous state"". None of Scott, Lee or Levy discloses such limitations. Scott in view of Lee was discussed above.

Levy describes a system for executing a software application. A plurality of hardware independent bytecodes is generated by a computing system. A virtual machine, in conjunction with a remote verification mechanism, cooperates to receive and execute the plurality of bytecodes. However, Levy fails to disclose the Trusted Dictionary "having an associated secure count…wherein each time the secure count is incremented during operation of the application, the trusted dictionary is placed into an irreversible state, such that the trusted dictionary cannot be placed into a pervious state by replacing a file associated with the trusted dictionary with an older version of the file…and further prevents changing of the trusted dictionary to the previous state". Accordingly, it is submitted that claims 6, 26, and 46 are patentable over Scott in view of Lee in further view of Levy.

In view of the foregoing, Applicants submit that Scott, Lee and Levy fail to teach or suggest each and every element of the claimed invention and are therefore wholly inadequate in their teaching of the claimed invention as a whole, fail to motivate one skilled in the art to do what the patent Applicants have done, fail to recognize a problem recognized and solved only by the present invention, fail to offer any reasonable expectation of success in combining the References to perform as the claimed invention performs, fail to teach a modification to prior art that does not render the prior art being modified unsatisfactory for its intended purpose, and disclose a substantially different invention from the claimed invention, and therefore cannot properly be used to establish a prima facie case of obviousness. Accordingly, Applicants respectfully request

reconsideration and withdrawal of this rejection under 35 U.S.C. §103(a), which rejection Applicants consider to be traversed.

Third Rejection Under 35 U.S.C. §103(a)

Claims 10-11, 30-31 and 50-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott Oaks (hereinafter referred as Scott) (Java Security May 2001 XP002321663) in view of Lee, et al. (hereinafter referred to as Lee) U.S. Pub No. 2002/0147763 A1 and further in view of Watson (hereinafter referred as Watson) US Pub. No. 2005/0204126 A1. Applicants respectfully traverse this rejection. Claims 10-11 depend from independent Claim 1, whereas Claims 30-31 depend from independent Claim 21 and Claims 50-51 depend from independent Claim 41. As indicated above, claims 1, 21 and 41 have been amended to recite, inter alia, a Trusted Dictionary "having an associated secure count…wherein each time the secure count is incremented during operation of the application, the trusted dictionary is placed into an irreversible state, such that the trusted dictionary cannot be placed into a pervious state by replacing a file associated with the trusted dictionary with an older version of the file…and further prevents changing of the trusted dictionary to the previous state". None of Scott, Lee or Watson discloses such limitations. Scott in view of Lee was discussed above.

Watson describes a software based environment for providing secured authentication of media downloaded from a network or loaded from a media player. The environment includes two peer-mode operating virtual machines provided in the form of a low-level virtual machine and a high-level virtual machine. The high-level virtual machine provides application-level functions such as user interfacing mechanisms and input/output. The low-level virtual machine provides decoding and decryption functions. However, Watson fails to disclose a Trusted Dictionary "having an associated secure count…wherein each time the secure count is incremented during operation of the application, the trusted dictionary is placed into an irreversible state, such that the trusted dictionary cannot be placed into a pervious state by replacing a file associated with the trusted dictionary with an older version of the file…and further prevents changing of the

trusted dictionary to the previous state". Accordingly, it is submitted that claims 10-11, 30-31 and 50-51 are patentable over Scott in view of Lee in further view of Watson.

In view of the foregoing, Applicants submit that Scott, Lee and Watson fail to teach or suggest each and every element of the claimed invention and are therefore wholly inadequate in their teaching of the claimed invention as a whole, fail to motivate one skilled in the art to do what the patent Applicants have done, fail to recognize a problem recognized and solved only by the present invention, fail to offer any reasonable expectation of success in combining the References to perform as the claimed invention performs, fail to teach a modification to prior art that does not render the prior art being modified unsatisfactory for its intended purpose, and disclose a substantially different invention from the claimed invention, and therefore cannot properly be used to establish a prima facie case of obviousness. Accordingly, Applicants respectfully request reconsideration and withdrawal of this rejection under 35 U.S.C. §103(a), which rejection Applicants consider to be traversed.

Accordingly, Applicants respectfully request reconsideration and withdrawal of these rejections under 35 U.S.C. §103(a), which rejection Applicants consider to be traversed.

If a communication with Applicant's Attorneys would assist in advancing this case to allowance, the Examiner is cordially invited to contact the undersigned so that any such issues may be promptly resolved.

The Commissioner is hereby authorized to charge any additional fees that may be required for this amendment, or credit any overpayment, to 09-0441.

In the event that an extension of time is required, or may be required in addition to that requested in a petition for extension of time, the Commissioner is requested to grant a petition for that extension of time that is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to the above-identified Deposit Account.

Respectfully submitted,

CANTOR COLBURN LLP
Applicant's Attorneys

By: /Greg O'Bradovich/

Greg O'Bradovich
Registration No: 42,945
Customer No. 67232

Address: 20 Church St, 22nd Floor, Hartford, CT 06103
Telephone: (860) 286-2929
Fax: (860) 286-0115